Off-print of Teleteknik, Engelsk Edition, Vol. III, 1959, No. 2.

A GENERATOR OF RANDOM NUMBERS*

H. Isaksson
Telecommunications Research Laboratory

With a view to the application of the Danish electronic digital computer (DASK) to the solution of traffic-theoretical problems, the Telecommunications Research Laboratory of Denmark has developed a generator of random numbers. The present paper gives a brief description of the principles of operation of the generator and mentions some of the underlying considerations. Utilizing the shot noise effect in a diode, the generator is capable of producing 5,000 binary digits per second. The random numbers generated have been subjected to various statistical tests for randomness, all of which gave satisfactory results.

DK 681.14–523.8

Introduction

In telephone exchanges, the most economical arrangement of trunks and switching equipment to carry the required volume of traffic can be determined on a purely mathematical basis, as experience has shown that the frequency and duration of the calls follow certain statistical distributions. This being so, it is possible to construct a stochastic model to describe any particular switching problem. Applying the classical calculus of probability, such a problem in terms of probabilities is converted into a problem in terms of functional equations, the solution of which is a purely mathematical problem.

A mathematical method, based on probability calculus, of determining the proportion of lost calls in a telephone system was first evolved by *A. K. Erlang*. He derived the fundamental *B*-formula for determining the grade of service of a simple or "full availability" group of switching devices, i.e., a switching stage whose trunks and/or selectors cooperate in such a way that any one incoming call has access to any one available outlet.

In modern telephone systems, however, there are numerous instances of less perfect cooperation, in that any one call has access to certain outlets only, as is the case e.g. when the number of outgoing trunks from a group of selectors is greater than the number of selector bank contacts, for which reason the trunks are connected to the selectors according to a so-called "grading scheme". Using this term in a wider sense, a variety of problems of limited availability groups may be collectively referred to as grading problems.

Erlang examined a theoretically very simple grading problem and derived an exact formula for determination of the loss of calls, the so-called "ideal grading formula", in which he considers a group of n trunks being offered a total traffic A from selectors with k bank contacts, so that the calls from any one selector have access only to k particular ones out of the n trunks in the group, always assuming that the traffic is distributed entirely at random over these n trunks. The probability of loss is then determined by Erlang's ideal grading formula.

The grading scheme commonly employed in automatic telephone systems is more complicated, involving the use of individual trunks and common trunks as shown in **Fig. 1**. Here, 9 trunks are distributed over 2 selector groups such that

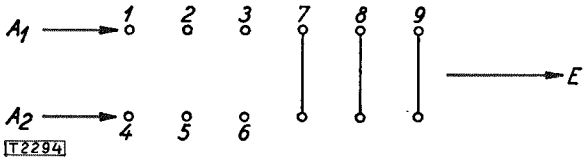

Fig. 1. Grading.

each selector group has access to 3 individual trunks (1—2—3 and 4—5—6), while the remaining 3 trunks (7—8—9) are shared by the two selector groups. The traffic offered by the two groups is A_1 erlang and A_2 erlang, respectively. *C. Palm* published, in 1936, the results of an exact calculation of some simple gradings of this type, but the formulas are not very well suited for numerical computation, for which reason an approximative method, suggested by *O'Dell*, is resorted to in most cases even though the approximation is fairly rough. Of course, the more complex the gradings, the greater the difficulties and the more incalculable the consequences of introducing approximations; and so it is only natural to seek other ways of solving grading problems.

*) This is a somewhat enlarged version of the original paper published in TELETEKNIK (Danish Edition), vol. IX, 1958, page 175.

A method frequently employed consists in making model experiments by means of what is known as traffic machines. These contain a number of electro-mechanical or electronic units which can be combined to form a model of the traffic system to be studied, and furthermore some means of generating an artificial traffic possessing specific statistical properties, supplemented with devices for measuring the respective volumes of traffic offered, completed, and lost. The desired empirical data on the traffic capacity of the telephone system in question can be obtained through a series of experiments with such a model.

In order to ensure sufficient accuracy it is necessary that a large number of calls be made for determination of any one point of measurement. Accordingly the traffic machines always operate with a greatly enlarged time scale so that, e.g., the amount of traffic handled during one hour in the real system will be handled during one minute in the model.

A major problem in the design of a traffic machine is how to produce the artificial traffic. Some practical solutions are based on purely mechanical methods (throwing of dice, Monte Carlo games of chance), while others depend on electrical phenomena (radioactive disintegration, thermionic noise or shot effect) as source of artificial traffic.

Many different traffic machines have been built during the last 25 years all over the world. These machines are often both large and expensive, and several of them come short in that they are designed for solution of a particular type of problem only and cannot readily be applied to other types of problems.

The development, during recent years, of the modern electronic digital computing machines quite naturally led to the idea of utilizing these for traffic experiments. A method of carrying out grading calculations according to the Monte Carlo system by means of the Swedish electronic computer BESK was first described by *Neovius* [1] in 1955. By this method, a simulated model of the system to be investigated is set up through a special programming of the computer, each switching device and its possible switching conditions being represented by memory cells in the storage section of the computer. The time intervals between successive calls are determined by means of a sequence of random numbers P_1, P_2, P_3, ... fed into the computer from some outside source, or generated by the computer itself. The random numbers, which will be uniformly distributed within a given interval, e.g. $0 < P < 1$, are transformed in the computing machine into another sequence of numbers S_1, S_2, S_3, ... in such a way as to produce the desired distribution of calls (the Poisson distribution, for example, is obtained by the transformation $S = -k \log_e P$). The holding times may be constant, or another sequence of suitably transformed random numbers may be employed to determine the holding times in accordance with a given distribution. In programming the computer, "instructions" can similarly be included as to the order in which the various groups of switching devices or trunks should be searched over.

Thanks to the great operating speed of the electronic computer, it permits traffic experiments by the method outlined above to be carried out at the same speed, or faster than by means of artificial traffic equipment proper. It is a requirement, however, that the random numbers can be generated quickly enough and in sufficient quantity.

The various available methods of generating random numbers can be divided into two fundamental categories: the mathematical and the physical methods.

Mathematical generation of random numbers is based on the experience that it is possible, by reiterating some simple algebraic operations, to produce a set of numbers whose terms may be regarded, with good approximation, as constituting a random sequence. These numbers will obviously be reproducible, a fact which may have certain advantages; thus, it enables one to watch closely the effects of a change in, say, a grading scheme, as the conditions of the experiment can otherwise be kept unchanged. Periodicity cannot possibly be avoided in these mathematically produced numbers, however; that is to say, one can only produce a finite quantity of numbers satisfying the condition of randomness.

In generating random numbers by physical methods, one utilizes natural phenomena having the characteristics of random occurrences. All atomic processes take a hap-hazard course as far as individual particles are concerned; examples are radioactive disintegration of atomic nuclei, and kinetic motions of electrons. Physically generated random numbers will in principle be nonperiodic, i.e., it is possible to produce an infinite quantity of random numbers.

For his traffic experiments on BESK, Neovius made use of random numbers generated by the computing machine itself according to methods that will be described at the end of the present paper. Taking cognizance of the Swedish experiments, the Danish telephone administrations — who for some time had been planning the construction of a traffic machine proper, to serve the purpose of solving grading-scheme problems — decided to abandon these plans and, instead, go in for applying to this purpose the Danish electronic digital computer DASK which was then in process of construction. At the same time, however, it was decided to build a special generator of random numbers, based on physical methods. This generator will be described in the following, and mention will be made of some of the considerations and experiments that led to the form of construction finally chosen. The last part of the paper gives the results of various statistical tests for randomness, applied to sequences obtained from the generator and to sequences obtained from the electronic computer utilizing the method employed by Neovius.

Physical Methods of Generating Random Numbers

Some examples of electronic generators of random numbers, as described in the literature, may be briefly mentioned here by way of introduction.

An electronic traffic analyser, constructed by the British G.P.O. and described by *Broadhurst* and *Harmston* [2], employs a generator of random numbers which utilizes the noise voltage from a neon tube. The machine contains a number of parallel-connected generators of this type, each generating 300 binary digits per second.

For use in connection with the German electronic computer "Göttinger Maschine G 2", a generator of random numbers has been designed which operates on the basis of radioactive radiation. The numbers are generated at the rate of 800 binary digits per second. Statistical tests, applied to sequences of length 7×10^5 bits, gave satisfactory results [3].

In the P.T.T. of Holland, *Kosten* [4] has developed a generator of random numbers with electrical noise as source. The operating principle deserves a brief mention, as it offers many advantages when the rate of speed, at which the numbers are to be generated, is a minor consideration. A free-running blocking oscillator is "frequency-modulated" by means of the noise from a noise diode, a noise voltage being superimposed upon the voltage on the grid of the oscillator. The moment at which the grid potential attains its cut-off value — i.e., at which the valve begins to draw current — can then be slightly accelerated or retarded by the superimposed noise voltage, to the effect that the time intervals between successive impulses from the blocking oscillator will be caused to vary at random about a mean value which equals the impulse period as for the undisturbed blocking oscillator. A count of the impulses from the blocking oscillator during a length of time which is great in relation to the mean impulse period, will be equally likely to reach an odd or an even total. The use of this arrangement ensures a certain minimum interval between the impulses to be counted, thus rendering the counter non-critical. The rate of output was in this case 50 bits per second.

Finally it may be mentioned that *Carl Jacobsen* [5] in some experiments, made at the Jutland Telephone Company with a simple type of traffic machine, has used a radioactive substance combined with a Geiger counter as source of artificial traffic.

Generator Based on Radioactive Disintegration

In attempting to generate random numbers by physical methods, the Telecommunications Research Laboratory first employed a method based on radioactive disintegration. **Fig. 2** illustrates the

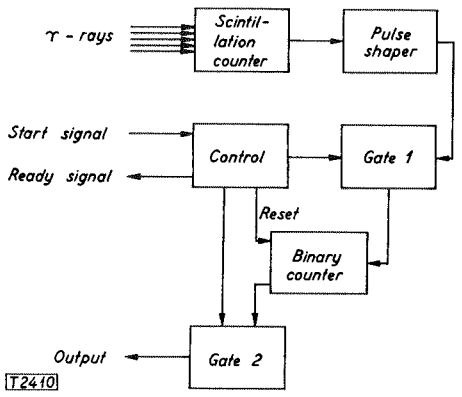

Fig. 2. Generation of random numbers based upon radioactive disintegration.

experimental apparatus, the operating principles of which are as follows: The γ-rays emitted from a radioactive substance are detected and converted into electric impulses, which are passed on to a counter that counts the number of impulses occurring during a given space of time.

Since the intervals between successive impulses are randomly distributed, it will be a matter of pure chance whether the number of impulses recorded by the counter during this space of time is even or odd. If the number is even, we shall say that the outcome is 0; if odd, the outcome is 1.

The γ-rays from the radioactive substance are converted into electric impulses by means of a scintillation counter, the impulses subsequently being amplified and shaped in a pulse shaper. Next, the impulses are routed via Gate 1 to the counter, which is a bistable multivibrator whose output signal is delivered via Gate 2. The whole process is controlled by a control device. Gates 1 and 2 are closed when the system is at rest. When a random number is to be generated, a starting impulse is applied to the control device, which then causes the following operations to take place in the order mentioned: Gate 1 is opened and kept open for a well-defined space of time, and the number of impulses received during that time is counted; on expiration of the counting period, a "ready"-signal is passed on to the electronic computer, which then reads the position of the counter via Gate 2; and finally the binary counter is reset. It is necessary to reset the counter at the end of each train of impulses so as to ensure exactly the same initial conditions for each random number generated, inasmuch as correlation between consecutive outcomes might otherwise be apt to result.

The impulses that are counted by the bistable multivibrator have different amplitudes, corresponding to the different amounts of energy of the several γ-particles, and the interval between any two impulses may sometimes be infinitesimally short. Since the bistable multivibrator inevitably has a certain relaxation period — i.e., it is insensitive to any disturbance for some time after it has counted an impulse — there will necessarily be instances of an impulse not being counted because it occurs too soon after the preceding one.

We shall now investigate theoretically how the relaxation period of the binary counter and the length of the counting period will affect the distribution of the numbers generated by this method, recognizing that, in order for these numbers to be random numbers proper, an equal distribution of 0 and 1 must be the first condition; or in other words, the outcomes 0 and 1 must be equally probable, as expressed by the equation $P(0) = P(1) = 1/2$.

Theoretical Study of the Distribution of 0 and 1 as for the Counting Method

For this purpose we set up a statistical model which represents, in principle, the generator of random numbers shown in Fig. 2. The underlying assumptions are:

1. That the mean distance between any 2 successive impulses from the scintillation counter is constant.
2. That the binary counter is reset to zero after each reading.
3. That the relaxation times of the binary counter on changing from Position 0 to Position 1, and from Position 1 to Position 0, are constant and equal to b and c times the mean impulse period, respectively.
4. That the interval from the time of resetting to zero until the time of reading (the counting period) is constant.
5. That impulses occurring during a relaxation period cannot operate the counter.

Without causing any change in the subsequently calculated probabilities, the requirements as to constant relaxation time and counting period may be replaced with a stipulation to the effect that they may follow distributions having the mean values b, c, and T, if only these distributions are independent of time.

If the mean impulse period is used as unit of time, the probability of no impulses occurring during the time interval dt will be

$$e^{-t}\,dt \qquad (1)$$

Let us now consider the time interval T, extending from the resetting of the counter at time $t = 0$ until the next reading of the counter at time $t = T$; and let us suppose that the multivibrator has been triggered altogether n times, viz.

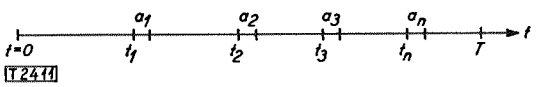

Fig. 3. Counting period with triggering times and relaxation periods.

the first time at time t_1, the second time at time t_2, and so on. These triggering times and the corresponding relaxation periods a_1, a_2, . . . a_n are marked off along the time axis shown in **Fig. 3**.

The probability of just this course of events, $p(t_1, t_2, \ldots, t_n, T)$, is the product of the following probabilities:

that the 1st impulse period is t_1
that the 2nd impulse period is $t_2 - t_1 - a_1$
that the 3rd impulse period is $t_3 - t_2 - a_2$
.....
that the nth impulse period is $t_n - t_{n-1} - a_{n-1}$

$a_\nu = b$ for ν odd
$a_\nu = c$ for ν even

and that no impulse occurs from time $t_n + a_n$ until time T.

For $t_n \geqq T - a_n$, this last-mentioned probability is 1, and for $t_n < T - a_n$ it is

$$\int_{(T-t_n-a_n)}^{\infty} e^{-t}\,dt = e^{-(T-t_n-a_n)}. \qquad (2)$$

Thus we have

$$p(t_1, t_2, \ldots, t_n, T) = \begin{cases} e^{-t_1} \times e^{-(t_2-t_1-a_1)} \times \ldots \times e^{-(t_n-t_{n-1}-a_{n-1})} \times e^{-(T-t_n-a_n)} & \text{for } t_n < T-a_n, \text{ and} \\ e^{-t_1} \times e^{-(t_2-t_1-a_1)} \times \ldots \times e^{-(t_n-t_{n-1}-a_{n-1})} & \text{for } t_n \geqq T-a_n, \text{ or} \end{cases}$$

$$p(t_1, \ldots, t_n, T) = \begin{cases} e^{-(T-\sum_1^n a_\nu)}, & t_n < T-a_n \\ e^{-(t_n-\sum_1^{n-1} a_\nu)}, & t_n \geqq T-a_n \end{cases} \qquad (3)$$

The probability $p(n)$ of the flip-flop being triggered n times within time T is then obtained by integrating $p(t_1, t_2, \ldots, t_n, T)$ over the interval of possible values of the n variables $(t_1, \ldots, t_n)$:

$$\sum_1^{\nu-1} a_\nu \leqq t_\nu \leqq t_{\nu+1} - a_\nu, \quad \nu = 1, 2, \ldots, n-1 \qquad (4)$$

$$\sum_1^{n-1} a_\nu \leqq t_n < T$$

The resulting n-tuple integral reduces to the simple integral

$$p(n) = \int_{\sum_1^{n-1} a_\nu}^{T} p(t_1, \ldots, t_n, T)\, \frac{(t_n - \sum_1^{n-1} a_\nu)^{n-1}}{(n-1)!}\, dt_n, \qquad (5)$$

$p(t_1, \ldots, t_n, T)$ being independent of the first $n-1$ variables $t_1, t_2, \ldots, t_{n-1}$.

Using (2) we obtain

$$p(n) = \int_{\sum_1^{n-1} a_\nu}^{T-a_n} e^{-(T-\sum_1^n a_\nu)}\, \frac{(t_n - \sum_1^{n-1} a_\nu)^{n-1}}{(n-1)!}\, dt_n$$

$$\int_{T-a_n}^{T} e^{-(t_n-\sum_1^{n-1} a_\nu)}\, \frac{(t_n - \sum_1^{n-1} a_\nu)^{n-1}}{(n-1)!}\, dt_n,$$

or

$$p(n) = e^{-(T-\sum_1^n a_\nu)}\, \frac{(T - \sum_1^n a_\nu)^n}{n!}$$

$$\int_{T-\sum_1^n a_\nu}^{T-\sum_1^{n-1} a_\nu} e^{-x}\, \frac{x^{n-1}}{(n-1)!}\, dx. \qquad (6)$$

Finally, expanding e^{-x} in a series and integrating term by term, we obtain

$$p(n) = e^{-(T-\sum_1^n a_\nu)}\, \frac{(T - \sum_1^n a_\nu)^n}{n!}$$

$$\sum_{\mu=0}^{n-1} e^{-(T-\sum_1^n a_\nu)}\, \frac{(T - \sum_1^n a_\nu)^\mu}{\mu!} -$$

$$e^{-(T-\sum_1^{n-1} a_\nu)}\, \frac{(T - \sum_1^{n-1} a_\nu)^\mu}{\mu!}. \qquad (7)$$

Now letting A denote the event of "an even number of changes" during the time T, the probability of a zero reading — i.e., "outcome 0" — will be $P(A)$. Assuming that the relaxation period is the same for either direction of triggering, which means that $c = b = a$, we find

$$P(A) = \sum_{\nu=0}^{\frac{T}{a}} (-1)^{\nu} \sum_{\mu=0}^{\nu} \frac{(T-\nu a)^{\mu}}{\mu!} e^{-(T-\nu a)}, \quad (8)$$

where

a is the relaxation time in terms of mean impulse periods, and

T is the interval from the time of resetting until the time of reading (the counting period).

By means of formula (8), $P(A)$ has been calculated for different values of T and a, and the values of the quantity $(P(A) - 1/2) \times 10^6$ evaluated on the basis thereof are listed in the following table:

T \ a	0	0.10	0.20	0.30	0.40	0.50
2	9158	5607				
4	167	62	11	0	—10	—237
8	0.056	1	1	—1	—1	0
12		1				

$$(P(A) - 1/2)10^6 = f(a, T)$$

In judging the worth of the above figures it should be borne in mind that the numerical evaluation of the separate terms of the summation was continued to six decimal places only.

The binary counter, as employed in the experimental apparatus under consideration, had a relaxation period of 0.4 microsecond. With a mean impulse period of 4 microseconds, the corresponding a-value is 0.1. It appears from the table that for this a-value, a counting period $T \geqq 8$ will give a skewness of less than 10^{-6} in the distribution of outcomes 0 and 1, which may be regarded as satisfactory.

For $T = 8$ and $a = 0.1$, there will be a skewness of 10^{-6} in favour of an even number of changes. Omission of resetting the binary counter to zero after each reading would cause the probability of the counter's position at the expiration of a counting period being the same as its initial position, to be different from 1/2; in fact, the probability would be $1/2 + 10^{-6}$, i.e., there would result a correlation between any two consecutive outcomes. Such correlation between the numbers produced is inconsistent with the second fundamental requirement in order for the numbers to be proper random numbers, viz., that any number in the sequence must be independent of all previous numbers.

If, on the other hand, the binary counter is reset to zero before each new counting period, the relaxation time will not give rise to any correlation; there will merely be a difference between the frequencies of 0 and 1, which, however, can be rendered insignificant by means of the artifice mentioned below (double game).

By way of verifying the above theory experimentally, an apparatus was built up in the laboratory as illustrated by the block diagram in Fig. 2. With the counting period T as variable quantity, a number of counts were then made at different mean impulse periods, and the experimentally determined skewnesses were compared with the theoretical values.

The results showed agreement between theoretical and experimental values for small values of T; for $T \geqq$ about 5, however, the experimentally determined skewness did not decrease as T was increased, but assumed a constant value of about 10^{-4}. This indicates that the laboratory apparatus in some respects differed essentially from the statistical model. The actual causes of this discrepancy were not investigated in detail, but it may have been due to any of the following circumstances: different sensitivity of the binary counter in the two directions of triggering, different periods of relaxation in the two directions of triggering, or different impulse lengths, all of which are circumstances that cannot possibly be kept under complete control in a practical model apparatus.

Double Game

However, the undesirable effects of the inevitable non-symmetry in the binary counter can be eliminated — providing that the non-symmetry is constant — by considering the generated digits two by two and stipulating that the combination 10 shall mean 0, and that 01 shall mean 1, while the combinations 00 and 11 shall be disregarded entirely.

If the probability of the outcome 1 in the simple game is $P(1) = 1/2 + \delta$, and the probability of 0 consequently is $P(0) = 1/2 - \delta$, then the probabilities of outcomes $P(01)$ and $P(10)$ in the double game will always be equally great, viz.,

$$P(01) = P(10) = P(0) \times P(1)$$
$$= (1/2 - \delta)(1/2 + \delta) = 1/4 - \delta^2.$$

Application of the double game will reduce the number of generated random bits to at most 1/4 of the corresponding number obtainable in the simple game, as the outcomes of the latter are combined in pairs, and as at least one half of these pairs are to be left out of consideration.

No double-game experiments were carried out in connexion with the above-described generator based on radioactive disintegration, as the rather highly radioactive substance that was necessary in order to ensure a sufficiently high impulse frequency called for such elaborate safety measures that it was decided to abandon this method in favour of using electrical noise as basis for the generation of random numbers.

Generator Based on Electrical Noise

Now, a more handy and harmless form of random physical phenomena is the electrical noise occurring either as thermal agitation noise in passive networks, or as shot effect in thermionic valves.

The thermal agitation noise in passive networks is due to the fact that electrons moving in electric conductors according to the kinetic theory have randomly distributed velocities, whose mean value depends on the absolute temperature. The shot effect in thermionic valves is due to the quantum-wise emission of electrons from the heated cath-

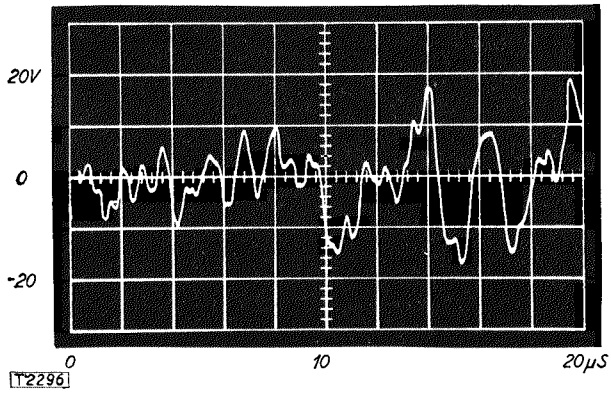

Fig. 4. Noise amplifier output voltage.

ode, and the fact that the separate electrons are emitted from the cathode at randomly distributed time intervals, in consequence of which the anode current will be subject to random variations. In **Fig. 4** is shown, by way of example, the noise voltage from a diode after it has been amplified in a wide-band amplifier whose upper limiting frequency is about 400 kc/s. Of these two kinds of electrical noise, the valve noise is the more advantageous, since it is more powerful and accordingly requires less amplification.

We shall now see how the noise voltage can be utilized as a source of random numbers. Several

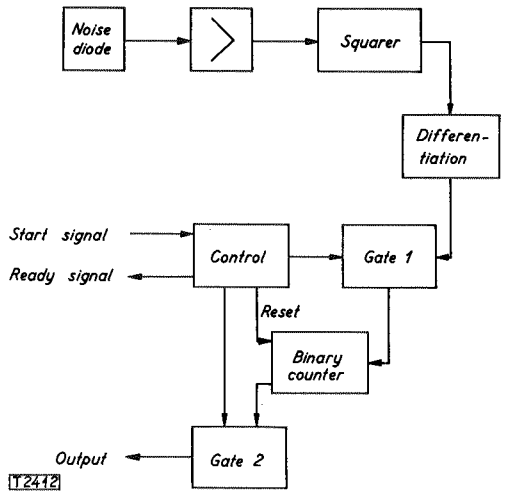

Fig. 5. Principle of the summation method.

methods are available, but we shall assume the following two methods to be representative of them all.

By the first, or *summation*, method we count the number of times that the noise voltage curve crosses the zero line in an upward direction (i.e., passes from a negative to a positive value) within a given time interval. If this number is even, we shall say that the outcome is 0; if odd, the outcome is 1. In order for the numbers thus obtained to be random numbers, it is necessary that the length of the given interval be great in comparison with the mean distance between the zero passages.

By the second, or *sampling*, method the signs of the noise voltage are read out at regular intervals. After amplification, the noise voltage is a pure a. c. voltage which varies about zero. The lengths of the intervals between the zero passages vary at random and are exponentially distributed; i.e., provided that the reading-out, or sampling, frequency is small as compared with the mean frequency of zero passages, it is a matter of pure chance whether the noise voltage will be positive or negative at the time of sampling.

The summation method can be applied in practice by means of the arrangement shown in **Fig. 5**. The noise voltage is amplified and changed into a voltage of square waveform, which is then differentiated. In accordance with the properties of the noise voltage, the positive (or negative) im-

pulses thus obtained will be randomly distributed and are consequently suitable for use in generating random numbers in exactly the same manner as described in the case of the radioactivity method.

A practical adaption of the sampling method is outlined in **Fig. 6**. Here, too, the noise voltage is amplified and changed into a voltage of square

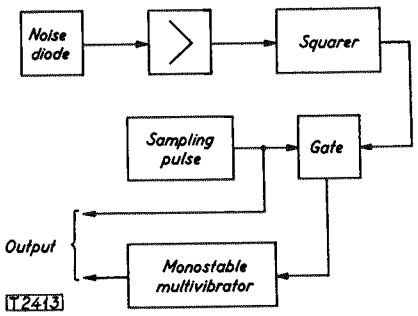

Fig. 6. Principle of the sampling method.

waveform. The polarity of the noise voltage is read out by means of a gate, controlled by a series of periodical sampling pulses, the period being τ. If the noise voltage is negative at the time of sampling, the square-wave voltage will also be negative, and the gate circuit will be blocked. If the noise voltage is positive, the square-wave voltage will be positive, and the gate circuit will be open, permitting the sampling pulse to pass through the gate and trigger the monostable multivibrator. The latter will thus produce a well-defined impulse every time the noise voltage is read out as being positive, while no impulse will appear when the noise voltage is read out as being negative. The two possible outcomes — impulse or no impulse — are taken as representing the two binary digits 1 and 0, respectively. In order for the condition $P(0) = P(1)$ to be satisfied, the conversion of the noise voltage into a voltage of square waveform should be quite ideal. Such ideal conversion not being achievable in actual practice, however, it is necessary to employ the double-game procedure in the case of the sampling method, too, so as to ensure an even distribution of the random numbers.

The first two devices involved in converting the noise voltage, viz., the noise amplifier and the square-wave generator, are thus common to the sampling method and the summation method. We shall therefore discuss in detail certain circumstances which are of consequence to the design of these devices.

Autocorrelation of the Noise Voltage

Let us first consider the sampling method. As previously mentioned, it is a condition for the randomness of the numbers generated that there should exist no significant correlation between the signs of the noise voltage as read out at any two consecutive times of sampling. Correlation will inevitably arise in the noise amplifier due to the finite bandwidth of the latter, and so it is necessary to determine the relationship between the frequency response of the noise amplifier and the ensuing autocorrelation.

An expression of the correlation arising between two consecutive readings taken at an interval of time τ is obtainable by means of the autocorrelation function

$$\psi(\tau)=\overline{x(t)x(t+\tau)}=\lim_{T\to\infty}\frac{1}{2T}\int_{-T}^{T}x(t)x(t+\tau)\,dt,$$

where $x(t)$ is a function of value + 1 when the noise voltage is positive, and of value — 1 when the noise voltage is negative.

Assuming the noise voltage of the diode to be ideal white noise, the autocorrelation in the amplified noise voltage will be determinable on the basis of our knowledge of the transfer function $A(\omega)$ of the amplifier. We have the following expression for the normalized autocorrelation [6]

$$\psi(\tau)_0=\frac{\int_0^\infty |A(\omega)|^2\cos\tau\omega\,d\omega}{\int_0^\infty |A(\omega)|^2\,d\omega}.$$

First we consider an amplifier whose transfer characteristic at high frequencies is given by

$$|A(\omega)|^2=\frac{1}{\left(1+\left(\frac{\omega}{\omega_0}\right)^2\right)^4},$$

i.e., a four-stage amplifier with the same time-constant $\frac{1}{\omega_0}=RC$ in all four stages. In this case the normalized autocorrelation will be

$$\psi(\tau)_0=e^{-\frac{\tau}{RC}}\left\{1+\frac{\tau}{RC}+0.4\left(\frac{\tau}{RC}\right)^2+0.07\left(\frac{\tau}{RC}\right)^3\right\}.$$

For small values of the autocorrelation, the latter will decrease exponentially as τ decreases.

In the second place we consider an amplifier of ideal band-pass filter qualities, its lower and

upper limiting frequencies being f_{inf} and f_{sup}. Here, the normalized autocorrelation function is given by the expression

$$\psi(\tau)_0 = \cos \pi\tau (f_{inf}+f_{sup}) \frac{\sin \pi\tau (f_{sup}-f_{inf})}{\pi\tau (f_{sup}-f_{inf})}.$$

For increasing values of τ, this function will pass through a succession of positive maxima and negative minima, the values of which will be nearly equal to $\frac{1}{\pi\tau (f_{sup}-f_{inf})}$, i.e., inversely proportional to τ.

Hence it appears that the *RC* type of amplifier offers the greatest advantage with respect to the autocorrelation of the amplified noise voltage, since $\psi(\tau)_0$ here decreases much more rapidly as τ increases.

To illustrate this point, the maximum values of $\psi(\tau)_0$ for $\tau = 5$ μsec and $\tau = 50$ μsec are tabulated below as for a four-stage *RC*-characteristic amplifier with $RC = 3.1 \times 10^{-7}$, corresponding to an upper limiting frequency (3 db down) of about 250 kc/s, and as for an ideal band-pass filter amplifier having a bandwidth of 70—400 kc/s.

τ μsec	*RC*-Amplifier $RC = 3.1 \times 10^{-7}$	Band-Filter Amplifier $f_{sup} = 400$ kc/s, $f_{inf} = 70$ kc/s
5	4×10^{-5}	2×10^{-1}
50	3×10^{-65}	2×10^{-2}

Normalized Autocorrelation for two Types of Amplifier.

It will appear from the table that the autocorrelation of the amplified noise voltage will be negligibly small in the case of the *RC* amplifier at $\tau = 50$ μsec, while in the case of the band-filter amplifier it will be impermissibly great. In recognition hereof, an *RC* amplifier of the said *RC* value, and with $\tau = 50$ μsec corresponding to a sampling-impulse frequency of 20 kc/s, was employed in the final construction of the generator of random numbers.

When the correlation between two consecutive readings-out is too great to be disregarded, the following relations can be shown [7] to be applicable in the case of the sampling method:

$$P(0-0) = P(1-1) = \frac{1}{4} + \frac{1}{2\pi}\psi(\tau)_0$$

$$P(1-0) = P(0-1) = \frac{1}{4} - \frac{1}{2\pi}\psi(\tau)_0,$$

where $P(0-0)$, $P(1-1)$, etc., are the probabilities that the outcomes of two consecutive readings-out will be 0,0, 1,1, etc., respectively. The expressions are valid only for $\psi(\tau)_0 \ll 1$ and $P(0) = P(1)$. [If $P(0) \neq P(1)$, the relations $P(0-0) = P(1-1)$ and $P(1-0) = P(0-1)$ will still hold good, but the deviation of the *P*-values from $\frac{1}{4}$ will be greater]. In other words, a positive correlation between two consecutive readings-out will manifest itself in a tendency for one outcome to be the same as the preceding outcome. In consequence of the fact that it is necessary, as already mentioned, to apply the double-game procedure and discard the outcomes $0-0$ and $1-1$, the correlation will not give rise to non-symmetry in the outcomes $1-0$ and $0-1$, which are written $0'$ and $1'$, respectively.

It can further be shown that

$$P(1-0-1-0) = P(0-1-0-1) = 4\left(\frac{1}{4} - \frac{1}{2\pi}\psi(\tau)_0\right)^3$$

and

$$P(0-1-1-0) = P(1-0-0-1) = 4\left(\frac{1}{4} - \frac{1}{2\pi}\psi(\tau)_0\right)^2\left(\frac{1}{4} + \frac{1}{2\pi}\psi(\tau)_0\right),$$

i.e., the probabilities $P(0'-0') = P(1'-1')$ will be different from the probabilities $P(1'-0') = P(0'-1')$. In the event of a significantly great positive correlation there will thus be a tendency for a double-game outcome ($0'$ or $1'$) to be different from the preceding outcome. A significant correlation can accordingly be ascertained by applying a frequency test to groups of two bits each, for the binary digits $0'$ and $1'$.

Correspondingly it can be shown [7] that when the summation method is employed, there will arise a similar correlation between the correlation in the noise and the outcomes of the counts, so that the correlation arising in the noise amplifier will influence the distribution of the random numbers equally much whether the sampling method or the summation method is used in producing the random numbers from out of the noise voltage.

With a view to the design of the various devices which are to "process" the noise voltage,

it is necessary to know how closely upon one another the zero passages may occur in the amplified noise voltage. An expression has been formulated [7] for the probability that the noise-voltage curve will cut the zero line while ascending, both during the interval $0 < t < dt$ and during the interval $\tau < t < \tau + dt$. This expression is a function of τ and is dependent on the frequency response of the amplifier. If the amplifier works as an ideal band-pass filter with upper limiting frequency f_{sup}, this expression will be equal to 0 for $0 < \tau < \frac{1}{f_{sup}}$; i.e., the noise voltage will not ascend through zero level at shorter intervals than $t_{min} = \frac{1}{f_{sup}}$. This is highly desirable with a view to the other devices in the set-up. On the other hand, if the frequency response of the amplifier corresponds to an *RC* cut-off curve, we arrive at another expression for the interval between zero-passages which is not equal to zero in the neighbourhood of the point $\tau = 0$; i.e., the impulses may occur one after another in arbitrarily rapid succession. As previously shown, considerations of autocorrelation necessitate the use of an amplifier of *RC* cut-off characteristics, and it is thus impossible to avoid having zero-passages occurring at infinitely short intervals. The rise time of the square-wave voltage should therefore be made as short as at all possible.

In the matter of choice of operating principle for the generator of random numbers it was finally decided to prefer the sampling method to the summation method, as the former permits one of the noise-voltage-processing devices to be dispensed with, viz., the differentiation unit; besides, the problem of the relaxation period of the counter is thus disposed of, inasmuch as the impulses to the monostable multivibrator by the sampling method will arrive at intervals which are whole multiples of τ.

The logical lay-out of the generator of random numbers will appear from the logical block diagram in **Fig. 7** and the impulse diagram in **Fig. 8.**

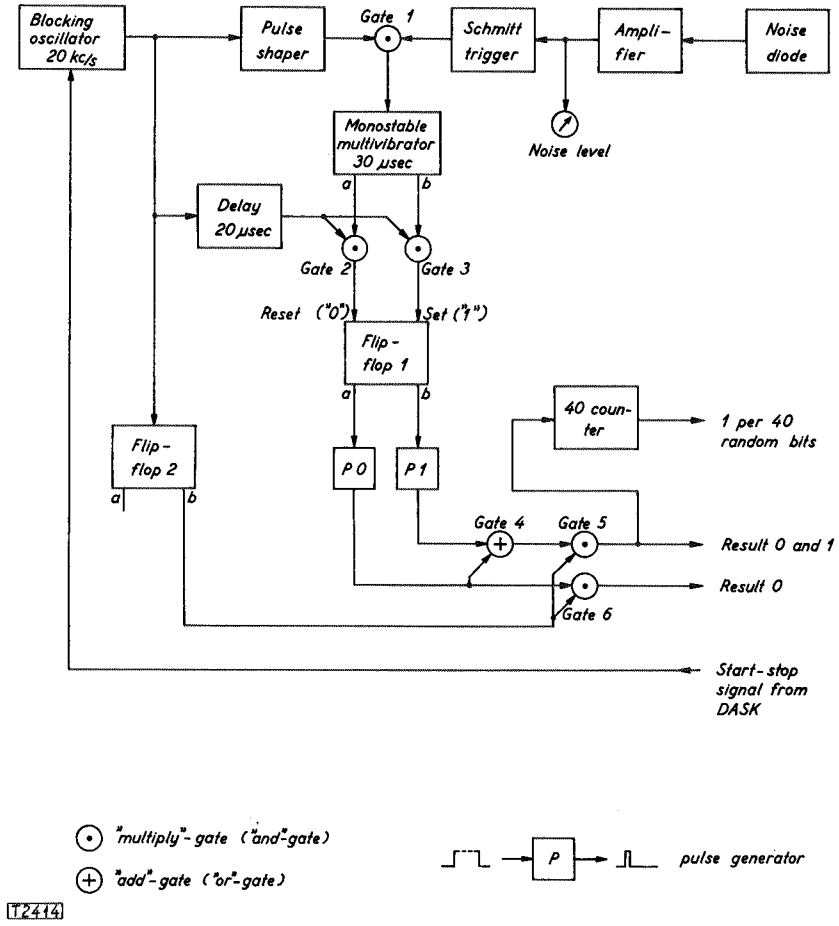

Fig. 7. Generator of random numbers. Block diagram.

The noise voltage is first amplified and then, in the Schmitt trigger, converted into a square-wave voltage, which is passed on to Gate 1. The sampling pulse, which is generated by means of a free-running blocking oscillator and a pulse shaper, is also passed on to Gate 1. Now if the output voltage from the Schmitt trigger is high, Gate 1 will be open to the sampling pulse which is positive, and a pulse will appear on the output terminals of Gate 1 (a multiply-gate). If, on the other hand, the square-wave voltage is low at the time when the sampling pulse occurs, the latter will find Gate 1 closed. The output pulse from sampled, the monostable multivibrator will be triggered, and the two inverse output signals will, for a period of 30 microseconds, hold Gate 2 open and Gate 3 closed, respectively. An impulse is applied to these two gates 20 microseconds after the sampling, and as only Gate 2 is open, this will have the effect of triggering Flip-Flop 1 into its 0-state if it is not already resting in that state. If the next sampling takes place at a time when the noise voltage is negative, the monostable multivibrator will not be triggered; i.e., only Gate 3 is open now, so that Flip-Flop 1 will be triggered into its 1-state by the delayed impulse appearing

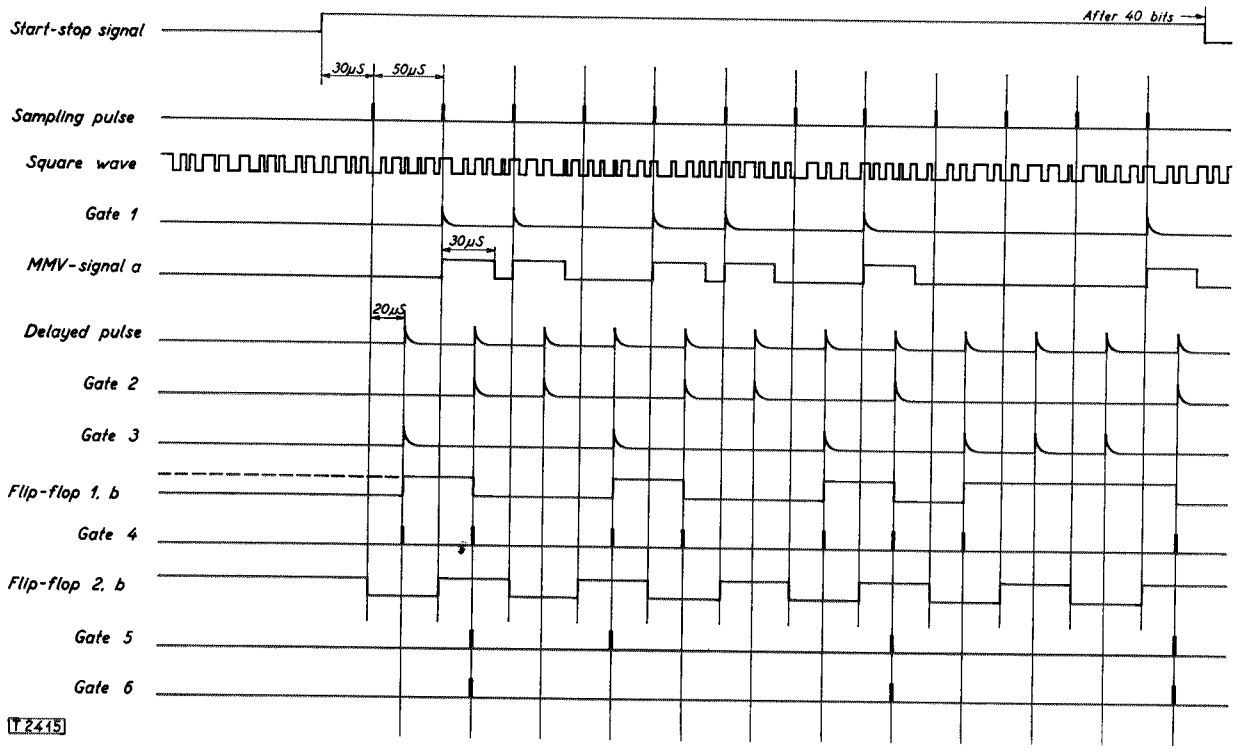

Fig. 8. Pulse diagram.

Gate 1 triggers a monostable multivibrator which remains triggered for 30 microseconds, i.e., for a shorter period than the interval between sampling pulses which is 50 microseconds. Thus the monostable multivibrator will be triggered only when the noise voltage is positive at the time of sampling.

As previously mentioned, it takes two consecutive samplings to generate one random number. The outcome of one sampling must therefore be stored in a memory until the outcome of the next sampling is available. This memory consists of Flip-Flop 1, whose two states of rest represent the two possible outcomes. The outcome of a sampling is passed on to Flip-Flop 1 by means of Gate 2 and Gate 3. If the noise voltage is positive when 20 microseconds after the sampling. Flip-Flop 1 is thus caused to change its state each time a sampling outcome is different from the one immediately preceding it. The two inverse output signals from Flip-Flop 1, which of course are d.c. signals, are converted into impulses by the pulse-forming networks P0 and P1; that is to say, P0 will generate a pulse when Flip-Flop 1 assumes its 0-state, while correspondingly P1 will generate a pulse when Flip-Flop 1 assumes its 1-state.

The sampling outcomes are to be combined in pairs, but in such a way as to prevent overlapping of the pairs. This is realized by the introduction of two multiply-gates, Gate 5 and Gate 6, which are controlled by Flip-Flop 2. The latter is trig-

gered by the sampling pulses, so that Gate 5 and Gate 6 will be open only in every second interval between sampling pulses. Gate 5 will pass a pulse when and if the generator has produced a random number; if, and only if, this random number is a zero, Gate 6 will pass a pulse, too.

The random numbers are to be fed into DASK in series of 40 bits each, and the generator assembly therefore incorporates a 40-counter which passes a signal to DASK each time a total of 40 digits has been generated. A starting signal from DASK will start the blocking oscillator, and when 40 random numbers have been generated, another signal from DASK will stop it.

Practical Construction of the Generator

All component circuits such as monostable and bistable multivibrators, gate circuits, Schmitt trigger, blocking oscillator, et cetera, were constructed on the usual general principles and dimensioned so as to satisfy the tolerances normally specified for computer circuits. The correct performance of the circuits will remain unaffected under conditions of ± 10 % resistance variations and a 50 % reduction of the thermionic emission in the valves.

Fig. 9 shows the generator in its final form of construction, consisting of three panels mounted on a standard 19" vertical rack. A total of 55 valves (not including those for the power supply unit) were used, most of which are of the types E 90 CC, E 80 L, and E 180 F.

The noise diode (K 81 A) and its associated amplifier are placed uppermost on the rack so as to render the shielding as effective as possible. In the frequency range of 70—250 kc/s the noise amplifier has a gain of 50.000, or 94 db, and the noise level is controlled by adjusting the filament current of the noise diode. Since it is essential that the noise voltage should not drop below a certain level, the panel is fitted with a diode voltmeter which directly indicates the noise level. The Schmitt trigger and Gate 1 are also mounted on the upper panel. The logical circuits are all mounted on the centre panel, while the lower panel carries a stabilized power supply unit which feeds all the sensitive circuits located on the upper panel. The remaining circuits are voltage-fed from DASK. Filament voltage for the noise diode is obtained from a 2-volt secondary cell.

On the panels, and accessible from the front of the rack, there is furthermore fitted a number of test jacks for use in making adjustments and control measurements, and an auxiliary device for checking the functioning of the logical circuits is also incorporated. Normally, however, no adjustments are needed in starting up the generator

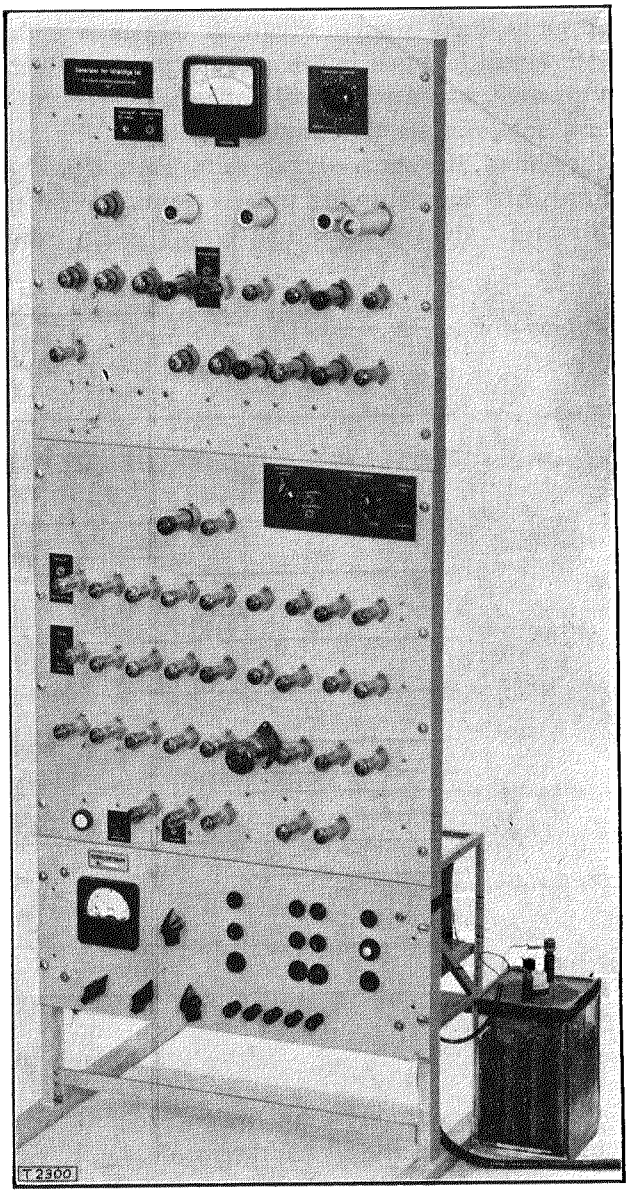

Fig. 9. Generator of random numbers.

which is done quite simply by closing the mains switch and turning on the noise-diode filament current. It is intended to publish a follow-up report in a later issue of TELETEKNIK when the generator has been used for a prolonged period of time.

Mathematically Produced Random Numbers

So as to make it possible to form an opinion of the "quality" of the random numbers obtained from the generator described in the foregoing, a

statistical investigation of two types of mathematically produced random numbers was carried out *pari passu* with an investigation of the numbers generated by the generator. From among the many well-known mathematical methods available, two methods were chosen which had previously been employed in connexion with some traffic experiments on BESK, the Swedish electronic computer [1].

These mathematical methods are both based upon the following modification of the Fibonacci sequence:

$$R_{n+1} = (R_n + R_{n-1}) \bmod 2^{40}.$$

In the case of the first of the methods under consideration, two independent number-sequences A and B are developed in accordance with the above formula. Every second number in the A-sequence is used in making up the random sequence proper, some of the digits at the beginning of the numbers however being omitted. The number of binary digits to be omitted is defined by b_n = the number consisting of the first four binary digits of every second B-number. The first 0 up to 15 digits of A can thus be omitted. The remaining digits are moved b_n places to the left so that, at any rate, the first 25 out of the 40 positions are occupied by random digits. Only the first 20 of these are used, the remaining positions being discarded. By repeating this procedure we fill up the last 20 positions, thereby obtaining a pseudo-random number of 40 digits.

This modification may be expressed in terms of the following formulas:

$$A_{n+1} = (A_n + A_{n-1}) \bmod 2^{40}$$

$$B_{n+1} = (B_n + B_{n-1}) \bmod 2^{40}$$

Method **b**: b_n = the number consisting of the first four digits of B_n

$$\begin{cases} R_n = 2^{b_n}(A_n) \bmod 2^{40-b_n} \\ n = \text{an even number} \end{cases}$$

The second method under consideration is based upon 17 random numbers of 40 digits, $C_0, C_1, C_2, \ldots C_{16}$, which are renewed gradually as the random numbers are produced. The initial values of the C-numbers may be taken from, e.g., a table of random numbers.

As in the case of the modification described above, two mutually independent sequences of random numbers, A-numbers and B-numbers, are developed. The first four binary digits a_n of every second A-number (n even) are used to define two consecutive C-numbers, C_{a_n} and C_{a_n+1}. If, say, $a_n = 0110 = 6$, the two C-numbers chosen will thus be C_6 and C_7.

These two numbers of the C-sequence are then replaced with C'_6 and C'_7:

$$C'_6 = (C_6 + C_7) \bmod 2^{40}$$

$$C'_7 = (C_7 + C'_6) \bmod 2^{40},$$

and C'_7 is chosen to be the next random number R_n, after omission of the first b_n binary digits, where b_n is the number consisting of the first four binary digits of every second B-number. Expressed in terms of formulas, the second modification may be written thus:

$$A_{n+1} = (A_n + A_{n-1}) \bmod 2^{40}$$

$$B_{n+1} = (B_n + B_{n-1}) \bmod 2^{40}$$

Method **c**:

$$C'_{a_n} = (C_{a_n} + C_{a_n+1}) \bmod 2^{40}$$

$$C'_{a_n+1} = (C_{a_n+1} + C'_{a_n}) \bmod 2^{40}$$

$$\begin{cases} R_n = 2^{b_n}(C'_{a_n+1}) \bmod 2^{40-b_n} \\ n = \text{an even number} \end{cases}$$

a_n = the number consisting of the first four digits of A_n

b_n = the number consisting of the first four digits of B_n

Thus, two out of the 17 C-numbers will be replaced each time a random number is produced.

In the experiments made with the aid of DASK, method **b** occupied storage space in the computer corresponding to 28 orders, and it took from a minimum of 37 and up to a maximum of 41 "addition times" (1 addition time = 56 microseconds) to produce 40 random digits, corresponding to 1 binary digit per 50 microseconds, approximately. Method **c** required storage space as for 72 orders, and a 40-digit number could be produced in from 59 to 63 "addition times" at a minimum and at a maximum, respectively.

It should be noticed that the mathematical methods here employed deviate from the methods described in [1], as *Neovius* only utilizes the first four binary digits of each of the 20-digit numbers used here.

Results of Statistical Investigations of Random Numbers as Obtained from the Generator Described, and as Produced Mathematically by Two Different Methods

The statistical investigations consist in application of the following four tests which were sug-

gested by *Kendall* and *Smith* [8], and which are commonly used as standard tests for the randomness of random numbers:

1. Frequency test
2. Frequency test on groups
3. Poker test
4. Gap test

These four tests will be described in detail below, the theoretical distributions will be stated, and the results of the tests will be compared with the theoretical distributions by means of the Chi-square test. A sequence of random numbers is said to fail a test when the χ^2-value corresponds to a probability which falls outside the interval

$$0.025 \leqq P(> \chi^2) \leqq 0.975.$$

These are the limits usually specified, but they are otherwise arbitrarily fixed. With this 5 per cent level of significance one will, in five out of a hundred cases on an average, in the event of agreement between the experimental and the theoretical distribution, be willing erroneously to reject a correct distribution.

1. *Frequency Test*

In the frequency test, the distribution of 0 and 1 is determined. In a sequence of N bits the number n of figures 1 are counted. The non-symmetry may then be expressed in terms of per mille of $\bar{n} = \frac{1}{2} N$ as

$$a = \frac{2n - N}{N} 10^3.$$

Now we produce A sequences of N bits each, wishing to determine the distribution of a. The theoretical value of the standard deviation in this distribution is

$$\sigma = \frac{10^3}{\sqrt{N}},$$

as a will follow the binomial distribution. The experimental value of the standard deviation is determined from the expression

$$s^2 = \frac{\sum_i a_i^2 p_i}{A},$$

where p_i denotes the number of times that a assumes the value a_i, and A is the total number of sequences.

Chi-square is determined from the expression

$$\chi^2 = \sum_i \frac{(p_i - \pi_i)^2}{\pi_i},$$

where p_i denotes the experimental frequencies, and π_i the ideal frequencies. The chi-square distribution is tabulated in the form of $\chi^2 = \chi^2(P, f)$, where P is the probability of χ^2 assuming a value greater than a given χ^2-value, and where f is the number of degrees of freedom equal to the number of classes minus the number of restraints imposed upon the theoretical frequencies π_i in fitting them to the observed frequencies. There is one restraint here, viz., the total number of outcomes.

The test was applied to $A = 200$ sequences, of $N = 10^5$ bits each, of the electronically generated numbers, and of the numbers produced mathematically by method **b**. The χ^2 value was determined as for a grouping into 16 class intervals. Good agreement with the theoretical distribution was found in both cases.

2. *Frequency Test on Groups*

A frequency test on groups is carried out by determining the relative frequencies of the 2^n different n-digit numbers. Thus, for groups of $n = 2, 3, 4, \ldots 8$ bits, respectively, the frequencies of the 4, 8, 16, ... 256 possible combinations of n bits are to be determined. For example, if $n = 2$, the possible outcomes are 00, 01, 10, and 11, each having the theoretical relative frequency of 0.25; in this case there are three degrees of freedom.

The procedure of testing was as follows: χ^2 was computed for N groups of n bits each, 30 times for each N- and n-value. The test was carried through for four N-values per n, with n assuming the values 2, 3, 4, ... 8, and with the ratio of n to N being so adjusted as to ensure that the theoretical number of outcomes within a group never is less than 10.

The physically generated numbers invariably showed good agreement with the theoretical distributions, whereas either type of mathematically produced numbers in one case (viz., for $n = 8$ and $N = 4000$) deviated substantially from the theoretical distribution, in that χ^2 departed from the 5 per cent level of significance in the case of 7 values out of 30 under Method **b** and 9 values out of 30 under Method **c**.

Frequency tests on groups were also applied to longer sequences, χ^2 being computed for the cumulated groups. The chi-square value was determined each time the total number of groups of n bits was increased by 50,000, $n = 2, 3, 4, \ldots 8$; for each n-value, the test was continued as far as to a total number of groups of approximately 10^6. Both the physically generated numbers and those produced mathematically by Method **b** showed good agreement with the theoretical distribution, while the numbers produced by Method **c** in one case (viz., for $n = 2$) exhibited a significant deviation.

3. *Poker Test*

The poker test is applied to groups containing 5 consecutive 4-digit binary numbers. These are divided into 6 classes:

AAAAA + AAAAB
AAABB
AAABC
AABBC
AABCD
ABCDE

where A, B, C, D, and E each can assume values ranging from 0000 to 1111, and where the ordering of the numbers within the group is indifferent. The first class is made up of two subgroups, whose respective probabilities are too small for the chi-square test to be applicable to them separately. The respective theoretical probabilities of the 6 classes are: $76(\frac{1}{16})^4$, $150(\frac{1}{16})^4$, $2100(\frac{1}{16})^4$, $3150(\frac{1}{16})^4$, $27300(\frac{1}{16})^4$, and $32760(\frac{1}{16})^4$.

The poker test procedure employed was the same as described for the frequency test on groups. χ^2 was determined 30 times for N groups of 5×4 bits, $N = 2400$ and $N = 5000$. Neither in the case of the physically generated numbers nor in the cases of the two types of mathematically produced numbers did χ^2 depart from the 5 per cent level of significance in more than 3 instances out of 30.

The poker test was also applied to longer sequences, χ^2 being computed for the cumulated numbers each time the total number of groups was increased by 5000. Altogether 2×10^5 groups of the three types of numbers were subjected to the test. The physically generated numbers and the mathematically produced numbers of Type **c** passed the test, while the mathematically produced numbers of Type **b** gave significant χ^2-values.

4. *Gap Test*

By the gap test, the distances between consecutive identical 4-digit binary numbers are determined. Different intervals ranging from 0 to 46 and intervals $\geqq 47$ are counted as for the 16 different 4-digit numbers, corresponding to a total of 48 classes.

The theoretical probability that consecutive identical 4-digit numbers will occur at intervals of n, is $2^{-4}(2^{-4} \times 15)^n$.

The gap test was likewise applied to 30 groups of N 4-digit numbers each, with N equal to 1700, 5000, and 10,000. For all three types of random numbers, χ^2 did not depart from the 5 per cent level of significance in more than 3 instances out of 30.

Finally, the gap test was applied to cumulated sequences, χ^2 being computed each time the number was increased by 10,000. The physically generated numbers exhibited significant chi-square values in one instance, as χ^2 dropped below the lower limit of significance. The terminal value of χ^2 was within the permissible limits, however. Repeated tests revealed no significant chi-square values. Method **b** yielded no significant chi-square values, while Method **c** gave significant values above and below the critical region for χ^2.

The above-mentioned results of tests applied to the mathematically produced numbers were all obtained by investigating the same random numbers; in other words, the initial values in the Fibonacci sequences were the same at the outset of all the tests. (The initial values were taken from a table of random numbers).

Conclusion

By a series of statistical tests it has been proved possible to design a generator of random numbers on the basis of electrical noise, the tests not having revealed any kind of systematism or periodicity in the numbers obtained from the generator. Similar tests concurrently applied to some pseudo-random numbers, produced mathematically by two different methods, revealed no correlation of any importance in these numbers, either.

However, as the mathematically produced random numbers are systematic in principle, even though this systematism was not disclosed by the tests, the situation may be envisaged that in the case of certain applications of the numbers, a result may issue which is fundamentally different from the result one would obtain by em-

ploying random numbers produced by some non-systematical method; and in actual practice it will be impossible to make sure that the systematism of the mathematically produced random numbers will not manifest itself in the results.

The fact that the mathematically produced numbers — unlike those generated by the physical method — are reproducible, is of minor importance now that the use of magnetic-tape memories in connexion with electronic computers permits very large quantities of bits to be stored. The conclusion from this is therefore that in many cases the random numbers obtained from the generator are to be preferred to the various types of pseudo-random numbers produced by mathematical methods.

Acknowledgements

The generator of random numbers, described in the foregoing, was developed at the Telecommunications Research Laboratory of Denmark under the direction of Professor J. Oskar Nielsen and supported financially by a Marshall Aid grant under Act 209 of June 7, 1952.

The work was actually started by the technical manager of the Danish Institute for Computing Machines, B. Scharøe-Petersen, B.Eng., who conducted a series of experiments on the use of radioactive disintegration as a source of random events. The probability-theoretical considerations upon which the design of this generator is based are due to Mr. Niels Ivar Bech, managing director of the same Institute. The coding of programmes for the mathematically produced random numbers and for the tests of randomness employed, and the planning of all the statistical investigations was done at the Institute for Computing Machines by Aage Melbye, B.Pol.Econ.

On behalf of the Telecommunications Research Laboratory, the author wishes to thank all those who have contributed to the development of this project.

Bibliography

[1] *G. Neovius:* Artificial Traffic Trials Using Digital Computers. Ericsson Technics, 1955, no. 2, p. 280.
[2] *S. W. Broadhurst & A. T. Harmston:* An Electronic Traffic Analyser. P.O.E.E.J., vol. 14, part 4, Jan. 1950.
[3] *Sebastian von Hoerner:* Herstellung von Zufallszahlen auf Rechnenautomaten. Zeitschr. angew. Math. Phys., vol. 8, 1957.
[4] *L. Kosten:* Electronical Chance Organs. Het PTT-Bedrijf, vol. iii, no. 4, 1951.
[5] *Carl Jacobsen:* Forsøg med elektronisk teletrafikmaskine. TELETEKNIK, 1954.
[6] *Van der Ziel:* Noise. Chapmann & Hall Ltd., London 1955.
[7] *T. Motooka & H. Yamashita:* On the Generation Method of Random Numbers. J. Inst. Elect. Engrs. Japan, no. 5, 1954.
[8] *Kendall & Smith:* Tables of Random Sampling Numbers. Tracts for Computers, xxiv, Cambridge 1951.